BUNDESREPUBLIK DEUTSCHLAND

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen: 103 46 007.1

Anmeldetag: 02. Oktober 2003

Anmelder/Inhaber: Siemens Aktiengesellschaft, 80333 München/DE

Bezeichnung: Kommunikationseinrichtung und Verfahren zum Einstellen einer Sicherheitskonfiguration einer Kommunikationseinrichtung

IPC: H 04 L 12/24

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 28. Oktober 2004
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Schäfer

A 9161
06/00
EDV-L

Beschreibung

Kommunikationseinrichtung und Verfahren zum Einstellen einer Sicherheitskonfiguration einer Kommunikationseinrichtung

Die Erfindung schafft eine Kommunikationseinrichtung sowie ein Verfahren zum Einstellen einer Sicherheitskonfiguration einer Kommunikationseinrichtung.

In einer heutzutage üblichen Kommunikationseinrichtung ist eine feste Sicherheitskonfiguration vorgesehen, die bei Installationen der Software in der Kommunikationseinrichtung eingestellt wird. Insbesondere "Persönliche Firewall"-Kommunikationseinrichtungen, die beispielsweise von den Firmen Symantec/Norton, Sygate oder ZoneLabs verfügbar sind, weisen feste Sicherheitskonfigurationen auf.

Eine mobile Kommunikationseinrichtung wie ein persönlicher digitaler Assistent (**P**ersonal **D**igital **A**ssistant, PDA) mit einer oder mehreren Kommunikationsschnittstellen, welche eingerichtet sind zur Drahtlos-Kommunikation oder zur Mobilfunk-Kommunikation wird üblicherweise in einer Vielzahl unterschiedlicher Einsatzumgebungen eingesetzt. Es ist wünschenswert, einen möglichst hohen Grad an Kommunikationssicherheit bei der Kommunikationseinrichtung zu gewährleisten, ohne jedoch den Benutzungskomfort unnötig einzuschränken.

In [1] ist beschrieben, dass in einer Kommunikationseinrichtung mehrere unterschiedliche Sicherheitskonfigurationen zur Auswahl stehen, und eine gewünschte, ausgewählte Sicherheitskonfiguration zur Einstellung der Kommunikationseinrichtung beziehungsweise der sicherheitsrelevanten Parameter im Rahmen der Kommunikation definiert werden können.
Gemäß [1] wird die jeweilige Sicherheitskonfiguration, mit der die Kommunikationseinrichtung betrieben wird, abhängig von einer aufgerufenen World Wide Web-Seite ausgewählt, d.h. es wird abhängig davon, ob ein Kommunikationsaufbau im Inter-

net, in einem lokalen Intranet, auf einer vertrauenswürdigen World Wide Web-Seite oder einer vertrauens-eingeschränkten World Wide Web-Seite zugegriffen wird, jeweils eine unterschiedliche Sicherheitskonfiguration ausgewählt, und mit dieser ausgewählten Sicherheitskonfiguration wird die jeweilige Kommunikation betrieben.

Im Rahmen des World Wide Web-Browserprogramms Netscape Communicator™ werden in einem persönlichen Profil eines Benutzers Einstellungen, Lesezeichen und archivierte Nachrichten für den jeweiligen Benutzer gespeichert. Ein persönliches Benutzerprofil ermöglicht es, dass mehrere Personen den World Wide Web-Browser Netscape Communicator™ verwenden können mit unterschiedlichen Konfigurationseinstellungen.

Somit wird das Profil eines Benutzers und auch eine Konfiguration der Kommunikationseinrichtung benutzerspezifisch definiert.

In [2] sind ein Verfahren und ein System beschrieben, bei denen eine Zugriffskontrolle vorgesehen ist, bei welcher Berechtigungen zum Zugriff von einem Aufenthaltsort des Benutzers abhängen davon, ob sich der Benutzer beispielsweise im lokalen Intranet befindet oder ob er sich über einen Dial-up-Zugang eingewählt hat.

Bei der Kommunikationseinrichtung gemäß [3] werden Anwendungen von einem "Kontext-Provider" Informationen bereitgestellt über den aktuellen Kontext der Kommunikationseinrichtung beispielsweise über den geographischen Aufenthaltsort der Kommunikationseinrichtung (dort bezeichnet als "Master World") oder aufgrund physischer oder logischer Einheiten mit einer spezifischen Sichtweise (dort bezeichnet als "Secondary World"), beispielsweise zur Unterscheidung von Standorten, Gebäuden, Stockwerken und Räumen eines Unternehmens.

Ferner ist in [4] eine Kommunikationseinrichtung beschrieben, bei der mehrere Benutzerschnittstellen definiert sind und abhängig von dem Aufenthaltsort des Benutzers beziehungsweise der Kommunikationseinrichtungen aktiviert werden. Gemäß [4] ist es vorgesehen, dass abhängig von einem aktuellen Aufenthaltsort der Kommunikationseinrichtung ein World Wide Web-Browserprogramm jeweils unterschiedliche Startseiten aufruft.

In [5] ist ferner für eine Kommunikationseinrichtung ein Treiber-Computerprogramm beschrieben, bei dem ein Benutzerprofil zur Einstellung von Kommunikationsnetz-Parametern, welche im Rahmen einer Kommunikation verwendet werden, einstellbar sind.

Der Erfindung liegt das Problem zugrunde, einen möglichst optimalen Sicherheitsgrad einer Kommunikation mittels einer Kommunikationseinrichtung zu gewährleisten ohne unnötige Benutzereinschränkungen zu schaffen.

Das Problem wird durch die Kommunikationseinrichtung sowie durch das Verfahren zum Einstellen einer Sicherheitskonfiguration einer Kommunikationseinrichtung mit den Merkmalen gemäß den unabhängigen Patentansprüchen gelöst.

Eine Kommunikationseinrichtung weist eine Einsatzumgebungs-Ermittlungseinrichtung, welche eingerichtet ist zum Ermitteln einer Einsatzumgebung, in der die Kommunikationseinrichtung eingesetzt ist, auf. Anschaulich ist die Einsatzumgebung der Ort, an dem sich die Kommunikationseinrichtung bei Aufbau beziehungsweise Wiederaufnahme einer Kommunikationsverbindung befindet.

Ferner weist die Kommunikationseinrichtung mindestens eine Kommunikationsschnittstelle auf, welche eingerichtet ist zur Kommunikation mit mindestens einer anderen Kommunikationseinrichtung.

Weiterhin ist in der Kommunikationseinrichtung ein Sicherheitskonfigurations-Speicher vorgesehen, in dem eine Mehrzahl unterschiedlicher Sicherheitskonfigurationen hinsichtlich des Betriebs der Kommunikationseinrichtung gespeichert sind.

Beispiele für unterschiedliche Einsatzumgebungen sind die eigene Firmenumgebung, eine fremde Firmenumgebung, die eigene Privatwohnung, die Privatwohnung eines bekannten Dritten, oder eines vieler unterschiedlicher öffentlicher Zugangsnetze, beispielsweise öffentliche Access Points.

In der in der Sicherheitskonfiguration angegebenen Informationen zur Definition der Sicherheitsmaßnahmen, welche im Rahmen der Kommunikationseinrichtung gewährleistet werden sollen, können grundsätzlich beliebige Informationen enthalten sein, insbesondere werden jedoch Parameter verwendet, welche beispielsweise in einer "Persönlichen Firewall" bereitgestellt werden, die die Kommunikation abhängig von dem Kommunikationspartner, den verwendeten Kommunikationsprotokollen, den zu verwendenden oder gewünschten Diensten, den verwendeten Computerprogrammen oder der Tageszeit einschränken können. Zusätzlich kann in einer Sicherheitskonfiguration auch Information gespeichert sein, welche nicht-sicherheitsrelevante Aspekte der Kommunikationseinrichtungen definiert.

In der Kommunikationseinrichtung ist ferner eine Sicherheitskonfigurations-Ermittlungseinrichtung vorgesehen, welche derart eingerichtet ist, dass unter Verwendung der ermittelten Einsatzumgebung, anders ausgedrückt unter Verwendung des ermittelten Aufenthaltsorts eine diesem Aufenthaltsort beziehungsweise dieser Einsatzumgebung zugehörige Sicherheitskonfiguration aus der Mehrzahl von Sicherheitskonfigurationen ermittelt wird. Ferner ist eine Steuerungseinrichtung, im Folgenden bezeichnet als Sicherheitskonfigurations-Einstelleinrichtung, vorgesehen, welche eingerichtet ist zum Einstellen der Sicherheitskonfiguration der Kommunikations-

einrichtung gemäß der von der Sicherheitskonfigurations-Ermittlungseinrichtung ermittelten Sicherheitskonfiguration.

Bei einem Verfahren zum Einstellen einer Sicherheitskonfiguration bei einer Kommunikationseinrichtung wird in einem ersten Schritt eine Einsatzumgebung der Kommunikationseinrichtung ermittelt, in welcher die Kommunikationseinrichtung eingesetzt wird. Anders ausgedrückt bedeutet dies, dass in dem ersten Schritt der Aufenthaltsort der Kommunikationseinrichtung ermittelt wird. Aus einer Mehrzahl in einem Sicherheitskonfigurations-Speicher der Kommunikationseinrichtung gespeicherter unterschiedlicher Sicherheitskonfigurationen hinsichtlich des Betriebs der Kommunikationseinrichtung wird unter Verwendung der ermittelten Einsatzumgebung eine zugehörige Sicherheitskonfiguration ermittelt, welche hinsichtlich der jeweiligen ermittelten Einsatzumgebung optimiert ist. Ist die zugehörige Sicherheitskonfiguration ermittelt, so wird die Kommunikationseinrichtung gemäß der ermittelten Sicherheitskonfiguration eingestellt, d.h. konfiguriert. Dies bedeutet, dass nach erfolgter Konfiguration der Kommunikationseinrichtung mit der ermittelten Sicherheitskonfiguration die Kommunikationseinrichtung eine Kommunikation gemäß den Vorschriften in der angegebenen ermittelten Sicherheitskonfiguration, durchführt.

Anschaulich kann die Erfindung darin gesehen werden, dass abhängig von der aktuellen Einsatzumgebung, d.h. abhängig von dem aktuellen Aufenthaltsort der Kommunikationseinrichtung die zu den Charakteristika der Einsatzumgebung gehörende Sicherheitskonfiguration in der Kommunikationseinrichtung aktiviert wird, so dass im Rahmen der Kommunikation der Kommunikationseinrichtung mit einer anderen Kommunikationseinrichtung an dem jeweiligen Einsatzort die dem Einsatzort optimiert angepasste Sicherheitskonfiguration verwendet wird.

Damit wird gewährleistet, dass abhängig von der Einsatzumgebung jeweils der maximale Grad an Sicherheit, der an der je-

weiligen Einsatzumgebung tatsächlich benötigt wird, gewährleistet wird und aufgrund der Anpassung der Sicherheitseigenschaften auch die Nutzerbeschränkungen nur so restriktiv gehandhabt werden, wie es unbedingt erforderlich ist bezogen auf die erforderliche Sicherheit in der jeweiligen Einsatzumgebung.

Bevorzugte Weiterbildungen der Erfindungen ergeben sich aus den abhängigen Ansprüchen.

Die folgenden Ausgestaltungen der Erfindung betreffen die Kommunikationseinrichtung und das Verfahren zum Einstellen einer Sicherheitskonfiguration einer Kommunikationseinrichtung.

Die Kommunikationseinrichtung ist vorzugsweise als mobile Kommunikationseinrichtung, insbesondere als zumindest eine der folgenden Kommunikationseinrichtungen eingerichtet:

- ein Mobilfunktelefon,
- ein Schnurlostelefon,
- ein persönlicher digitaler Assistent (Personal Digital Assistent, PDA),
- ein Pager, oder
- ein tragbarer Computer, beispielsweise ein Notebook-Computer.

Die einzelnen Kommunikationseinrichtungen beziehungsweise die einzelnen Funktionalitäten und Charakteristika der Kommunikationseinrichtungen können selbstverständlich in beliebiger Weise miteinander kombiniert in einer Kommunikationseinrichtung zusammengefasst sein.

Gemäß einer anderen Ausgestaltung der Erfindung ist es vorgesehen, dass die Kommunikationsschnittstelle eingerichtet ist

- als eine Kommunikationsschnittstelle zur Kommunikation mit einem Personal Computer (PC),
- als eine Modem-Kommunikationsschnittstelle,

- als eine ISDN-Adapter-Kommunikationsschnittstelle, und/oder
- als eine LAN-Adapter-Kommunikationsschnittstelle.

In diesem Fall ist die Kommunikationsschnittstelle üblicherweise eine kabelgebundene Kommunikationsschnittstelle, d.h. eine Kommunikationsschnittstelle, welche zur drahtgebundenen Kommunikation mit einem anderen Gerät beziehungsweise mit einer anderen Kommunikationseinrichtung eingerichtet ist.

In dem Fall, in dem die Kommunikationsschnittstelle zur Kommunikation mit einem Personal Computer eingerichtet ist, ist die Kommunikationsschnittstelle eine serielle Kommunikationsschnittstelle oder eine Parallel-Kommunikationsschnittstelle, beispielsweise eine USB-Kommunikationsschnittstelle. Ist die Kommunikationsschnittstelle eingerichtet als eine LAN-Adapter-Kommunikationsschnittstelle, so kann diese beispielsweise ein Adapter für einen LAN-Anschluss, beispielsweise für ein Internet-Kommunikationsnetz, oder ein Token Ring-Kommunikationsnetz sein.

Alternativ oder zusätzlich ist es gemäß einer anderen Ausgestaltung der Erfindung vorgesehen, dass die Kommunikationsschnittstelle oder eine andere Kommunikationsschnittstelle, welche zusätzlich in der Kommunikationseinrichtung vorgesehen ist, als Funk-Kommunikationsschnittstelle ausgestattet ist.

Vorzugsweise ist die Kommunikationsschnittstelle eingerichtet als:

- eine Wireless-LAN-Kommunikationsschnittstelle,
- eine Schnurlos-Kommunikationsschnittstelle, und/oder
- eine Mobilfunk-Kommunikationsschnittstelle.

Für den Fall, dass die Kommunikationsschnittstelle eine Wireless-LAN-Kommunikationsschnittstelle ist, kann sie gemäß dem Kommunikationsstandard 802.11 eingerichtet sein oder als Ho-

me-RF-Kommunikationsschnittstelle, alternativ als Bluetooth-Kommunikationsschnittstelle.

Eine Schnurlos-Kommunikationsschnittstelle ist beispielsweise eingerichtet zur Kommunikation gemäß dem DECT-Standard, dem CT2-Standard, dem PHS-Standard oder dem PACS-Standard.

Als Mobilfunk-Kommunikationsschnittstelle kann eine Kommunikationsschnittstelle vorgesehen sein, welche eingerichtet ist beispielsweise gemäß dem GSM-Standard, dem GPRS-Standard, dem UMTS-FDD-Standard, dem UMTS-TDD-Standard, dem CDMA-Standard, dem AMPS-Standard, dem DAMPS-Standard oder dem CDPD-Standard.

Gemäß einer anderen Ausgestaltung ist in der Kommunikationseinrichtung zusätzlich ein Zuordnungstabellen-Speicher vorgesehen, in dem eine Zuordnungstabelle gespeichert ist. In der Zuordnungstabelle ist zu einer Einsatzumgebung jeweils mindestens eine Sicherheitskonfiguration, welche zu der jeweiligen Einsatzumgebung optimierte Kommunikations-Sicherheits-Parameter definiert, zugeordnet.

In diesem Fall wird die Ermittlung der Sicherheitskonfiguration zu einer entsprechenden ermittelten Einsatzumgebung unter Verwendung der in dem Zuordnungstabellenspeicher gespeicherten Zuordnungstabelle ermittelt.

Gemäß einer anderen Ausgestaltung der Erfindung ist es vorgesehen, dass die Einsatzumgebungs-Ermittlungseinrichtung eine Einsatzumgebungs-Erfassungseinrichtung aufweist, die eingerichtet ist zum automatischen Erfassen und Bestimmen der Einsatzumgebung der Kommunikationseinrichtung. Vorzugsweise ist die Einsatzumgebungs-Erfassungseinrichtung eingerichtet zum Erfassen eines oder mehrerer von der Kommunikationseinrichtung verwendeter Kommunikationsverfahren und/oder zum Erfassen eines oder mehrerer von der Kommunikationseinrichtung im Rahmen einer Kommunikation verwendeter Sicherheitsmechanismen oder Sicherheitsmaßnahmen.

Auf diese Weise ist es auf sehr bedienerfreundliche Weise möglich, ohne Einbindung des Benutzers der Kommunikationseinrichtung, die jeweils optimiert angepassten und erforderlichen Sicherheitsparameter im Rahmen der Kommunikation der Kommunikationseinrichtung zu verwenden.

Alternativ ist es jedoch möglich, eine Vielzahl von unterschiedlichen Einsatzumgebungen einem Benutzer zur Auswahl darzustellen und die erfolgte Auswahl zu verwenden zur Ermittlung der für die ausgewählte Einsatzumgebung zugeordneten Sicherheitskonfiguration. In diesem Fall ist die Einsatzumgebungs-Ermittlungseinrichtung beispielsweise eine Tastatur oder ein anderes Eingabemedium zur Eingabe von Information in die Kommunikationseinrichtung. Beispielsweise kann auf einem Touchscreen eine Mehrzahl von Einsatzumgebungen einem Benutzer der Kommunikationseinrichtung dargestellt werden und der Benutzer tippt in diesem Fall lediglich mit einem Auswahlstift oder mit einem Finger auf den Ort des Touchscreens, an dem die gewünschte Einsatzumgebung dargestellt ist. Diese Eingabe wird erkannt und auf diese Weise wird die gewünschte Einsatzumgebung ermittelt.

Gemäß einer anderen Ausgestaltung der Erfindung ist es vorgesehen, dass die Einsatzumgebungs-Erfassungseinrichtung eingerichtet ist zum Erfassen eines oder mehrerer von der Kommunikationseinrichtung im Rahmen einer Kommunikation verwendeter Sicherheitsmechanismen, wobei zumindest einer der folgenden Sicherheitsmechanismen berücksichtigt wird:

- ein Authentisierungsverfahren,
- eine Identifizierungsinformation zur Identifikation einer Kommunikationseinrichtung oder eines Teilnehmers, d.h. eines Benutzers der Kommunikationseinrichtung,
- ein Schlüsselaustauschverfahren zum Austauschen kryptographischer Schlüssel, welches beispielsweise zum Aufbau einer Kommunikationsverbindung mittels der Kommunikationseinrichtung verwendet wird,

- einen im Rahmen der Kommunikation mittels der Kommunikationseinrichtung verwendeten kryptographischen Schlüssel, und/oder
- weitere im Rahmen der Kommunikation verwendete Informationselemente, beispielsweise kryptographisch basierte Zertifikate, Tickets, Credentials, usw.

Die Sicherheitsmechanismen, allgemein die Sicherheitsmaßnahmen, können für eine Kommunikationsschnittstelle beziehungsweise für ein gemäß der Kommunikationsschnittstelle zu verwendendes Kommunikationsprotokoll, wie oben verwendet, spezifisch sein. Sie können jedoch auch gemäß einem Kommunikations-Schichtenmodell auf höheren Kommunikationsprotokoll-Schichten erfolgen, beispielsweise bei einer Windows-Netzwerkanmeldung, bei einem PPP-Authentisierungsverfahren (EAP-Varianten, PAP, CHAP) oder beim Anmelden auf einer World Wide Web-Seite.

Die Einsatzumgebungs-Erfassungseinrichtung kann derart eingerichtet sein, dass zumindest eine der folgenden Einsatzumgebungen berücksichtigt werden kann beziehungsweise zur Auswahl durch einen Benutzer bereitgestellt werden kann, wobei der jeweiligen Einsatzumgebung jeweils mindestens eine Sicherheitskonfiguration zugeordnet ist:

- ein eigenes Firmen-Kommunikationsnetz,
- ein fremdes Kommunikationsnetz,
- das Heimat-Kommunikationsnetz eines Benutzers,
- das Heimat-Kommunikationsnetz eines Dritten,
- das öffentliche Kommunikationsnetz, und/oder
- ein Ad-Hoc-Kommunikationsnetz.

In einer Sicherheitskonfiguration können gemäß Ausgestaltungen der Erfindungen Informationen über zumindest einen Teil der folgenden Aspekte enthalten sein:

- Informationen über eines oder mehrere von der Kommunikationseinrichtung nutzbarer Kommunikationsprotokolle,

- Informationen über einen oder mehrere von der Kommunikationseinrichtung erreichbare Ziel-Kommunikationseinrichtungen, beispielsweise Ziel-Computer, mit denen die Kommunikationseinrichtung eine Kommunikationsverbindung aufbauen will,
- Informationen über von der Kommunikationseinrichtung ausführbare oder aufrufbare Computerprogramme oder Computerprogramm-Funktionen,
- Informationen über im Rahmen der Kommunikation von der Kommunikationseinrichtung zu verwendende Sicherheitsverfahren,
- Informationen über von der Kommunikationseinrichtung zugreifbare Daten,
- Informationen über von der Kommunikationseinrichtung gleichzeitig nutzbare Kommunikationsverfahren,
- Informationen über für die Kommunikationseinrichtung zugelassene Sicherheitsverfahren,
- Informationen über für die Kommunikationseinrichtung verbotene Sicherheitsverfahren und/oder
- Informationen über für die Kommunikationseinrichtung erforderlichen Sicherheitsverfahren.

Als zu verwendende Sicherheitsverfahren sind insbesondere Verfahren zur Netzwerkanmeldung, zu verwendende kryptographisch gesicherte Protokolle wie IPSec oder SSL/TLS, geeignet.

Eine jeweilige Aktivierung einer Sicherheitskonfiguration in der Kommunikationseinrichtung kann in einem Ereignisprotokoll, welches ebenfalls in einem Speicher der Kommunikationseinrichtung gespeichert sein kann, festgehalten werden. Anders ausgedrückt bedeutet dies, dass gemäß dieser Ausgestaltung der Erfindung die jeweilige Einstellung der Veränderung der Sicherheits-Betriebsparameter der Kommunikationseinrichtung gemäß der ausgewählten Sicherheitskonfiguration in einem Ereignisprotokoll festgehalten wird.

Die aktivierte, d.h. ermittelte Sicherheitskonfiguration kann ferner auf einer Ausgabeeinheit der Kommunikationseinheit oder einer externen Ausgabeeinheit einem Benutzer angezeigt werden. Ferner kann/können, wie oben erläutert, eine oder mehrere ermittelte beziehungsweise zur Auswahl dargestellte Einsatzumgebungen auf einer Ausgabeeinheit der Kommunikationseinrichtung oder einer externen Ausgabeeinheit, an welche die Kommunikationseinrichtung angeschlossen ist, einem Benutzer angezeigt werden. Die Ausgabeeinheit kann als "normaler" Bildschirm, beispielsweise als Flüssigkristall-Anzeige oder auch als Plasma-Anzeigeeinheit ausgestaltet sein, allgemein als jede beliebige elektronische Anzeigeeinheit, auf der einem Benutzer Daten angezeigt werden können.

Anschaulich kann die Erfindung darin gesehen werden, dass es nunmehr durch die erfindungsgemäße Kommunikationseinrichtung beziehungsweise durch das erfindungsgemäße Verfahren ermöglicht wird, die für eine Anwendungsumgebung passende Sicherheitskonfiguration eines Kommunikationsgerät beziehungsweise einer Kommunikationseinrichtung auszuwählen und zu aktivieren. Insbesondere aus Sicherheitssicht ergeben sich somit gravierende Vorteile, da unterschiedliche Einsatzumgebungen unterschiedliche Schutzmaßnahmen erfordern, wie oben erläutert wurde. Ein eigenes Heimat-Kommunikationsnetz oder ein eigenes Firmen-Kommunikationsnetz stellt eine geschützte Benutzerumgebung dar, in der deutlich geringere Schutzmaßnahmen akzeptabel sind als in einer "feindlichen Benutzerumgebung", wie es beispielsweise ein öffentlicher Internet-Zugang zu einem öffentlichen Kommunikationsnetz darstellt. Die damit verbundene Problematik, welche durch die Erfindung gelöst wird, wird zukünftig verstärkt auftreten, wenn tragbare Kommunikationseinrichtungen, insbesondere solche mit Drahtlos-Kommunikationsschnittstellen oder Mobilfunk-Kommunikationsschnittstellen vermehrt in unterschiedlichen Benutzerumgebungen eingesetzt werden.

Ferner trägt die Erfindung dazu bei, dass vorhandene Schutzmaßnahmen wie eine Firewall nicht durch mobile Kommunikationseinrichtungen oder Kommunikationsgeräte mit einer Funk-Kommunikationsschnittstelle wirkungslos gemacht werden. Grundsätzlich könnte ein Kommunikationsgerät, das an ein firmeninternes Intranet angeschlossen ist, über eine zweite, beispielsweise Drahtlos-Kommunikationsschnittstelle oder Mobilfunk-Kommunikationsschnittstelle einen Kommunikationsnetzübergang darstellen, der nicht durch eine vorhandene Firewall abgesichert ist. Durch eine der jeweiligen Benutzerumgebung angepasste Sicherheitskonfiguration, gemäß welcher die jeweilige Kommunikationseinrichtung betrieben wird, kann eine solche Kommunikationsschnittstelle deaktiviert werden. Auf diese Weise wird der Grad der verfügbaren Sicherheit optimiert.

Ausführungsbeispiele der Erfindung sind in den Figuren dargestellt und werden im Folgenden näher erläutert.

Es zeigen

Figur 1 eine Skizze einer Kommunikationseinrichtung gemäß einem ersten Ausführungsbeispiel der Erfindung;

Figur 2 ein Ablaufdiagramm, in dem einzelne Verfahrensschritte eines Verfahrens gemäß einem Ausführungsbeispiel der Erfindung dargestellt sind;

Figur 3 eine Skizze einer Kommunikationseinrichtung gemäß einem zweiten Ausführungsbeispiel der Erfindung.

Fig.1 zeigt einen Persönlichen Digitalen Assistenten (PDA) 100 als Kommunikationseinrichtung.

Der PDA 100 weist eine Antenne sowie eine oder mehrere Kommunikationsschnittstellen auf, welche als drahtgebundene Kommunikationsschnittstelle oder als Drahtlos-

Kommunikationsschnittstelle ausgestaltet ist/sind (nicht gezeigt).

Der PDA 100 weist hierfür vorzugsweise mindestens eine der folgenden Kommunikationsschnittstellen auf:

- ein Funkmodul für Wireless-LAN (beispielsweise gemäß dem Standard 802.11 oder gemäß HomeRF),
- ein Funkmodul für Schnurlos-Kommunikation (beispielsweise gemäß dem DECT-Standard, dem CT2-Standard, dem PHS-Standard oder dem PACS-Standard);
- ein Funkmodul für zellulären Mobilfunk (beispielsweise gemäß dem GSM-Standard, dem GPRS-Standard, dem UMTS-FDD-Standard, dem UMTS-TDD-Standard, dem CDMA-Standard, dem AMPS-Standard, dem DAMPS-Standard, dem CDPD-Standard);
- eine Schnittstelle zur direkten Kommunikation mit einem PC, eingerichtet als Seriell-Schnittstelle und/oder als Parallel-Schnittstelle, beispielsweise als USB-Schnittstelle;
- eine Modem-Kommunikationsschnittstelle;
- eine ISDN-Adapter-Kommunikationsschnittstelle; und/oder
- einen Adapter für einen LAN-Anschluss, beispielsweise für ein Internet-Kommunikationsnetz oder ein Token Ring-Kommunikationsnetz.

Ferner weist der PDA 100 nicht gezeigte Tasten zur Eingabe von Informationen auf, alternativ oder zusätzlich ein Touchscreen, d.h. eine berührungssensitive Anzeigeeinheit zur Ausgabe und Eingabe von Informationen an einen beziehungsweise durch einen Benutzer sowie eine Schnittstelle zur Verbindung an ein Energieversorgungsnetzwerk.

Ferner sind Steuertasten vorgesehen zum Steuern des Verhaltens des PDA 100.

Weiterhin weist der PDA 100 eine Konfigurationseinheit auf, vorzugsweise eingerichtet als Mikroprozessor, mittels der

Kommunikationsparameter, insbesondere sicherheitsrelevante Kommunikationsparameter des PDA 100 bestimmt werden.

Mittels der sicherheitsrelevanten Kommunikationsparameter wird jeweils festgelegt, wie die Kommunikation mittels des PDA 100 abzulaufen hat, insbesondere welche Sicherheitsaspekte und Sicherheitsmaßnahmen berücksichtigt und gewährleistet werden müssen. Die jeweiligen Sicherheitsaspekte und Sicherheitsmaßnahmen werden im Folgenden näher erläutert.

Ferner sind in der Konfigurationseinheit 101 eine Mehrzahl von Speichern vorgesehen, wobei die Mehrzahl von Speichern auch als ein gemeinsamer Speicher realisiert sein können, wobei der Speicher für die jeweils unterschiedlichen zu speichernden Daten eigene Speicherbereiche aufweist.

In einem ersten Speicher 102 beziehungsweise in einem ersten Speicherbereich 102 ist eine im Folgenden noch näher erläuterte aktuelle Einsatzumgebung, d.h. der aktuelle Aufenthaltsort des PDA 100 gespeichert.

Ferner ist in einem zweiten Speicher beziehungsweise in einem zweiten Speicherbereich eine Zuordnungstabelle 103 gespeichert, mittels der zu einer vorgegebenen jeweiligen Einsatzumgebung mindestens eine im Folgenden noch näher erläuterte Sicherheitskonfiguration gespeichert ist.

In einem dritten Speicher beziehungsweise in einem dritten Speicherbereich ist ein Computerprogramm gespeichert, welches derart eingerichtet ist, dass es, wie im Folgenden noch näher erläutert wird, die sicherheitsrelevanten Kommunikationsparameter des PDA 100 zur Einstellung der im Rahmen einer Kommunikation zu verwendenden Kommunikationsparameter einstellen kann.

Ferner sind in einem vierten Speicher beziehungsweise in einem vierten Speicherbereich n ($n = 1, 2, \ldots, m$, wobei mit m

die maximale Anzahl der gespeicherten Sicherheitskonfigurationen angegeben wird) Sicherheitskonfigurationen 105, 106, 107 gespeichert.

Gemäß dem ersten Ausführungsbeispiel der Erfindung ist der PDA 100 derart eingerichtet, dass seine aktuelle Einsatzumgebung, d.h. sein aktueller Aufenthaltsort, automatisch ermittelt werden kann. Dies erfolgt gemäß diesem Ausführungsbeispiel dadurch, dass die im Rahmen einer Kommunikation jeweils aktuell verwendeten Kommunikationsverfahrens beziehungsweise Kommunikationsprotokolle und die jeweils einzusetzenden Sicherheitsmaßnahmen, welche ein Kommunikationspartner im Rahmen eines Kommunikationsverbindungsaufbaus einsetzen möchte, erfasst und erkannt werden.

Als Erkennungsmerkmale werden gemäß dem Ausführungsbeispiel der Erfindung die jeweils verwendete Netzwerk-Kommunikationsschnittstelle, die verwendeten Kommunikations-Anmeldeverfahren, das zum Kommunikationsaufbau beziehungsweise zum Anmelden einer Kommunikationsverbindung verwendete Authentisierungsverfahren und die dabei verwendeten kryptographischen Schlüssel, eine Identifizierungsinformation beispielsweise eine Identifizierungsinformation, mittels der die Identität eines Netzzugangpunktes (Access Point) oder eine Netzbetreiberidentifizierung und/oder eingesetzte Sicherheitsverfahren wie beispielsweise der Aufbau einer VPN-Kommunikationsverbindung (Virtuelles Privates Netz) zu einem Netzzugangs-Serverrechner und die dabei verwendeten Parameter (Identifizierungsinformation, kryptographische Schlüssel, Authentisierungsverfahren) verwendet. Eine Einsatzumgebung kann auch durch den Aufenthaltsort des Kommunikationsgeräts bestimmt sein, der unter Verwendung eines Dienstes ermittelt wird, wie er in [3] beschrieben ist. Alternativ kann ein solcher Aufenthaltsort (wie in [3] beschrieben durch einen Dienst bereitgestellt) ein Erkennungsmerkmal darstellen, das zusammen mit weiteren Erkennungsmerkmalen ausgewertet wird, um die aktuelle Einsatzumgebung zu ermitteln.

Beispielsweise bei einer Wireless-LAN-Kommunikationsschnittstelle besteht die Möglichkeit, innerhalb eines eigenen Firmen-Kommunikationsnetzes, in einem Wireless-LAN-Kommunikationsnetz einer anderen Firma, in einem öffentlichen Internet-Zugang, beispielsweise auf einem Flughafen, in einem Hotel oder auch in einer Konferenz, oder in einem Heimat-Kommunikationsnetz des Benutzers des PDA oder in einem Heimat-Kommunikationsnetz einer anderen Person zu kommunizieren.

Ist in dem PDA 100 zusätzlich eine Kommunikationsschnittstelle vorgesehen zur direkten Kommunikationsverbindung mit einem Personal Computer, um beispielsweise unter dessen Verwendung den Datenbestand des PDA 100 mit dem in einem Personal Computer gespeicherten Datenbestand zu synchronisieren, ist selbstverständlich auch der Zugang zu einem Rechner-Kommunikationsnetz ermöglicht.

In den beschriebenen Ausführungsbeispielen der Erfindung sind vier Einsatzumgebungen berücksichtigt, welche in der Zuordnungstabelle 103 gespeichert sind und welchen jeweils eine Sicherheitskonfiguration, welche im Folgenden noch näher erläutert werden, zugeordnet ist.

In den Ausführungsbeispielen sind folgende vier Einsatzumgebungen berücksichtigt:

- Wireless-LAN-Einsatzumgebung innerhalb eines eigenen Firmenkommunikationsnetzes;
- Drahtgebundene Kommunikationsschnittstelle zu einem Personal Computer in einem eigenen Firmen-Kommunikationsnetz;
- eine Heimat-Kommunikationsnetz-Einsatzumgebung, d.h. einer Einsatzumgebung, bei sich der PDA 100 in den Heimat-Kommunikationsnetz des Teilnehmers eines Mobilfunk-Kommunikationsnetzes befindet; und
- eine sonstige Einsatzumgebung, d.h. eine Einsatzumgebung, die alle restlichen Fälle welche durch die oben

drei vorgesehenen Einsatzumgebungen nicht abgedeckt sind, beschreibt.

Gemäß diesen Ausführungsbeispielen sind in einer Sicherheitskonfiguration folgende Aspekte definiert:

- Filterregel für zugelassenen Daten-Netzverkehr, insbesondere bezogen auf eine Ziel-Rechneradresse, auf eines oder mehrere zu verwendender Kommunikationsprotokolle oder auf verfügbare digitale Dienste;
- eine Angabe darüber, ob eine Daten-Synchronisation ungesichert oder über eine gesicherte Kommunikationsverbindung erfolgen muss;
- eine Angabe über die Aufrufbarkeit einer Computeranwendung zum Zugriff auf eine firmeninterne Datenbank zur Projektverwaltung; und
- Aufrufbarkeit des Spiels "FallendeKlötzchen".

Allgemein ist zu bemerken, dass jede beliebige sicherheitsrelevante Information beziehungsweise Einstellung im Rahmen einer Kommunikationsverbindung in einer Sicherheitskonfiguration definiert sein kann.

Eine Konfiguration besteht in den dargestellten Beispielen aus einer Menge von Regeln, die in Pseudo-Code angegeben sind. Eine Sicherheitskonfiguration 105, 106, 107 kann in einer alternativen Ausführungsform über eine graphische Benutzerschnittstelle, über eine Datenbank (Registry) oder im Allgemeinen über beliebige andere Konfigurationsmechanismen definiert werden und in dem vierten Speicher beziehungsweise in dem vierten Speicherbereich des PDA 100 eingespeichert werden.

Im Folgenden sind die vier vorgesehenen Sicherheitskonfigurationen in Pseudo-Code dargestellt.

```
[Firma-Wireless]
ERLAUBE-NETZWERK = BELIEBIG
```

```
VERBIETE-PROGRAMME = c:\Programme\FallendeKlötzchen
ERLAUBE-PROGRAMME = BELIEBIG
ERLAUBE-SYNCHRONISATION = ABGESICHERT

[Firma-DirektPC]
ERLAUBE-NETZWERK = SCHNITTSTELLE(SERIELL, USB)
VERBIETE-PROGRAMME = c:\Programme\FallendeKlötzchen
ERLAUBE-PROGRAMME = BELIEBIG
ERLAUBE-SYNCHRONISATION = BELIEBIG

[Heim]
ERLAUBE-NETZWERK = BELIEBIG
VERBIETE-PROGRAMME = c:\Programme\ProjektVerwaltung
ERLAUBE-PROGRAMME = BELIEBIG
ERLAUBE-SYNCHRONISATION = KEINE

[Rest]
ERLAUBE-NETZWERK = SERVICE(HTTP, HTTPS)
VERWENDE = Content-Filter
VERBIETE-PROGRAMME = c:\Programme\ProjektVerwaltung
ERLAUBE-PROGRAMME = BELIEBIG
ERLAUBE-SYNCHRONISATION = KEINE
```

Gemäß der Sicherheitskonfiguration [Firma-Wireless] bestehen keine Einschränkungen, d.h. es ist ein beliebiger Kommunikationsnetz-Datenverkehr zugelassen ("ERLAUBE-NETZWERK = BELIEBIG"). Bis auf das Programm "c:\Programme\FallendeKlötzchen" können beliebige Computerprogramme von dem PDA 100 ausgeführt werden ("VERBIETE-PROGRAMME = c:\Programme\FallendeKlötzchen und "ERLAUBE-PROGRAMME = BELIEBIG"). Eine Synchronisation, d.h. ein Abgleich von in dem PDA 100 gespeicherten Daten (gespeicherte Adressen, Termine, Notizen) mit einem Synchronisationsgerät, beispielsweise einem angeschlossenen Personal Computer oder einem Synchronisationsserver-Rechner, darf gemäß dieser Sicherheitskonfiguration nur abgesichert erfolgen ("ERLAUBE-SYNCHRONISATION = ABGESICHERT").

Die Sicherheitskonfiguration [Firma-DirektPC] unterscheidet sich von der Sicherheitskonfiguration [Firma-Wireless] bezüglich des ersten Eintrags "ERLAUBE-NETZWERK = SCHNITTSTELLE(SERIELL, USB)". Dieser Eintrag bedeutet, dass eine Kommunikationsnetz-Verbindung gemäß dieser Sicherheitskonfiguration nur über eine serielle Kommunikationsschnittstelle oder über eine USB-Kommunikationsschnittstelle möglich ist. Dies kann sinnvoll sein, um sicherzustellen, dass das Kommunikationsgerät beziehungsweise der PDA 100 nicht als Gateway-Rechner arbeitet zwischen einem internen Firmen-Kommunikationsnetz (Intranet) und einem externen Kommunikationsnetz, welches über eine andere Kommunikations-Schnittstelle, beispielsweise über eine Wireless-LAN-Kommunikationsschnittstelle erreichbar ist. Durch diesen Eintrag werden alle Kommunikationsschnittstellen bis auf eine in dem PDA 100 gegebenenfalls enthaltene serielle Kommunikationsschnittstelle und eine ebenfalls gegebenenfalls enthaltene USB-Kommunikationsschnittstelle deaktiviert. Bezüglich der Synchronisation von gespeicherten Daten bestehen gemäß dieser Sicherheitskonfiguration keine Einschränkungen ("ERLAUBE-SYNCHRONISATION = BELIEBIG").

Gemäß der Sicherheitskonfiguration [Heim] bestehen bezüglich der zugelassenen Kommunikationsnetz-Verbindungen keine Einschränkungen ("ERLAUBE-NETZWERK = BELIEBIG"). Es sind alle Computerprogramme bis auf das Computerprogramm "c:\Programme\ProjektVerwaltung" zugelassen ("VERBIETE-PROGRAMME = c:\Programme\ProjektVerwaltung" und " ERLAUBE-PROGRAMME = BELIEBIG"). Eine Synchronisation, d.h. ein Datenabgleich von in dem PDA 100 gespeicherten Daten mit den Daten in einem Personal Computer oder mit einem Synchronisations-Serverrechner, allgemein mit einem Synchronisationsgerät, ist gemäß dieser Sicherheitskonfiguration nicht gestattet ("ERLAUBE-SYNCHRONISATION = KEINE").

Gemäß der Sicherheitskonfiguration [Rest] bestehen allerdings starke Einschränkungen bezüglich des Kommunikationsnetz-Datenverkehrs. Es sind nur die Netzwerkdienste HTTP (Hypertext Transfer Protokoll) und HTTPS (Hypertext Transfer Protokoll über Secure Socket Layer (SSL)) zugelassen ("ERLAUBE-NETZWERK = SERVICE(HTTP, HTTPS)"). Es ist zwingend vorgeschrieben einen "Content-Filter" zu verwenden, welcher verdächtige geladene Inhalte, d.h. in den PDA 100 geladene Daten, abblockt (beispielsweise gefährliche oder potentiell gefährliche World Wide Web-Inhalte, welche einen Computervirus enthalten könnten, die einen Computerwurm darstellen könnten oder die sonstige Schadensfunktionen ausführen könnten) (siehe "VERWENDE = Content-Filter"). Es dürfen beliebige Programme bis auf das Computerprogramm "c:\Programme\ProjektVerwaltung" aufgerufen werden ("VERBIETE-PROGRAMME = c:\Programme\ProjektVerwaltung" und "ERLAUBE-PROGRAMME = BELIEBIG"). Gemäß dieser Sicherheitskonfiguration ist keine Synchronisation von Daten zugelassen ("ERLAUBE-SYNCHRONISATION = KEINE").

Gemäß den beschriebenen bevorzugten Ausführungsbeispielen werden die Sicherheitskonfigurationen durch einen Benutzer des PDA 100 definiert.

In einer Ausführungsform ist es vorgesehen, auf einer Anzeigeeinheit des PDA eine Benutzeroberfläche darzustellen mit einer Schaltfläche, mittels welcher eine Änderung von Aktivierungsregeln, d.h. eine Änderung einer jeweiligen Sicherheitskonfiguration, ermöglicht ist.

Ferner ist es alternativ vorgesehen, dass ein Administrator die Sicherheitskonfigurationen einmalig definiert und nur er die Sicherheitskonfigurationen überhaupt ändern darf. Ein "normaler" Benutzer des PDA 100 hat keine Zugriffsrechte zur Änderung der gespeicherten Sicherheitskonfigurationen.

Ferner ist es vorteilhafterweise vorgesehen, dass die jeweils aktuelle Sicherheitskonfiguration mit der der PDA 100 eine Kommunikationsverbindung betreibt, und/oder die bekannte Einsatzumgebung, dem Benutzer des PDA visuell mittels der Anzeigeeinheit angezeigt werden/wird. Außerdem kann die Aktivierung einer Sicherheitskonfiguration in einem Ereignisprotokoll, welches ebenfalls in einem Speicher des PDA 100 gespeichert wird, festgehalten werden.

Gemäß dem ersten Ausführungsbeispiel wird somit die aktuelle Einsatzumgebung des Persönlichen Digitalen Assistenten automatisch erkannt und es folgt eine ebenfalls automatische Aktivierung der der Einsatzumgebung zugeordneten Sicherheitskonfiguration.

Das Erkennen der aktuellen Einsatzumgebung wird vorzugsweise durch Regeln definiert. Im Folgenden ist beispielhaft eine Liste von Regeln in einem Pseudo-Code-Format dargestellt.

Im dargestellten Ausführungsbeispiel beziehen sich die Regeln auf die Kommunikationsschnittstelle und die Eigenschaften der verwendeten Kommunikation (Kommunikationsnetz-Einstellungen), konkret auf die verwendete VPN-Definition und die Identität eines direkt an den PDA 100 angeschlossenen Computers. Die aktuelle Einsatzumgebung 102 ist in diesem Fall durch die abfragbaren Eigenschaften gegeben, d.h. durch die Angaben "Kommunikationsschnittstelle" und "Kommunikationsnetz-Einstellung". Die Zuordnung von Einsatzumgebung zu der jeweiligen Sicherheitskonfiguration ist durch die dargestellten Regeln definiert und in der Zuordnungstabelle 103 gespeichert. Diese Regeln werden von einer Zuordnungsfunktion, d.h. von einem in dem PDA gespeicherten Computerprogramm 103 ausgewertet.

```
IF Schnittstelle = WLAN and Kommunikationsnetz-Einstellung =
VPN-Firma THEN
     SET Sicherheitskonfiguration = Firma-Wireless
```

```
ELSE IF (Kommunikationsschnittstelle = seriell OR Kommunika-
tionsschnittstelle = USB) AND Peer = FirmaPC7123 THEN
     SET Sicherheitskonfiguration = Firma-DirektPC
ELSE IF Kommunikationsschnittstelle = WLAN AND Kommunikati-
onsnetz-Einstellung = myHomeNetwork THEN
     SET Sicherheitskonfiguration = Heim
ELSE IF (Kommunikationsschnittstelle = seriell OR Kommunika-
tionsschnittstelle = USB) AND Peer = myHomePC THEN
     SET Sicherheitskonfiguration = Heim
ELSE
     SET Sicherheitskonfiguration = Rest.
```

Die Sicherheitskonfiguration [Firma-Wireless] soll somit aktiviert werden, wenn der PDA 100 mittels der Wireless-LAN-Kommunikationsschnittstelle "WLAN" mit dem Firmen-Kommunikationsnetz verbunden ist. Die Kommunikation ist in diesem Fall über ein virtuelles privates Kommunikationsnetz (VPN-Firma) abgesichert.

Die Sicherheitskonfiguration [Firma-DirektPC] soll dagegen aktiviert werden, wenn der PDA 100 direkt mit dem Firmen-Personal Computer "FirmaPC7123" verbunden ist.

Die Sicherheitskonfiguration [Heim] soll aktiviert werden, wenn der PDA 100 sich über die Wireless-LAN-Kommunikationsschnittstelle "WLAN" in dem Heimat-Kommunikationsnetz des Benutzers befindet oder wenn der PDA direkt über die serielle Kommunikationsschnittstelle oder über die USB-Kommunikationsschnittstelle mit dem Heim-Personal Computer "MyHomePC" verbunden ist.

In allen anderen Fällen soll gemäß diesen Ausführungsbeispielen der Erfindung die Sicherheitskonfiguration [Rest] aktiviert werden.

Die Regeln zur Erkennung der Einsatzumgebung werden im dargestellten Beispiel durch den Benutzer des Kommunikationsgeräts, d.h. des PDA 100, definiert.

Es ist in einer alternativen Ausführungsform der Erfindung vorgesehen, dass ein Administrator diese Regeln definiert, wobei diese Einstellungen von einem Benutzer des PDA 100 nicht geändert werden können.

In einer alternativen Ausführungsform der Erfindung wird an Stelle oder zusätzlich zu dem bereits oben angeführten Regeln der aktuelle Aufenthaltsort des PDA 100 umfasst. Vorzugsweise wird der Aufenthaltsort in vorgegebenen definierten Kategorien angegeben, beispielsweise "Eigenes Büro", "Firmengelände", "Zuhause" statt in geographischen Angaben zu Längengrad und Breitengrad. Vorzugsweise erfolgt die Erfassung des Aufenthaltsorts gemäß dem in [3] beschriebenen Verfahren.

Im Folgenden sind gemäß diesem Ausführungsbeispiel drei Aufenthaltsort-Bereiche "Eigenes Büro", "Firmengelände" und "Zuhause" vorgegeben. Die Zuordnung von einer dieser Aufenthaltsort-Bereiche zu einer Sicherheitskonfiguration verfolgt durch Regeln, beispielsweise gemäß den im Folgenden Pseudo-Code angegebenen Regeln:

```
IF AktuellerOrt = EigenesBüro, THEN
     SET Sicherheitskonfiguration = Firma-DirektPC
ELSE IF AktuellerOrt = Firmengelände THEN
     SET Sicherheitskonfiguration = Firma-Wireless
ELSE IF AktuellerOrt = Zuhause THEN
     SET Sicherheitskonfiguration = Heim
ELSE
     SET Sicherheitskonfiguration = REST.
```

Bei diesen Regeln würde die Sicherheitskonfiguration [Firma-DirektPC] aktiviert, wenn das Kommunikationsgerät, d.h. gemäß diesem Ausführungsbeispiel der Erfindung der PDA 100, sich im

eigenen Büro des Benutzers befindet. Falls der PDA 100 sich nicht im eigenen Büro des Benutzers aber auf dem Firmengelände der eigenen Firma befindet, wird die Sicherheitskonfiguration [Firma-Wireless] aktiviert. Falls andernfalls sich der PDA 100 zu Hause beim Benutzer befindet, wird die Sicherheitskonfiguration [Heim] aktiviert. In allen anderen Fällen wird die Sicherheitskonfiguration [Rest] aktiviert.

Mittels der Konfigurationsfunktion 104 wird nach erfolgter Ermittlung der jeweiligen Einsatzumgebung und damit der passenden Sicherheitskonfiguration das Kommunikationsgerät, gemäß diesem Ausführungsbeispielen der PDA 100 gemäß der ermittelten Sicherheitskonfiguration 105, 106, 107 konfiguriert.

Fig.2 zeigt in einem Ablaufdiagramm 200 den Verfahrensablauf zur Ermittlung und Konfiguration des PDA 100.

Nach Start (Schritt 201) des Verfahrens wird von dem PDA 100 dessen aktuelle Einsatzumgebung ermittelt (Schritt 202).

In einem nachfolgenden Schritt (Schritt 203) wird unter Verwendung der Zuordnungsfunktion 103, welche von dem Mikroprozessor ausgeführt wird, die zu der aktuellen ermittelten Einsatzumgebung zugehörige Sicherheitskonfiguration ermittelt.

Anschließend wird die ermittelte zugehörige Sicherheitskonfiguration aktiviert, d.h. das Kommunikationsgerät wird mittels der Konfigurationsfunktion 104 ausgeführt, wodurch die Sicherheits-Kommunikationsparameter des PDA 100 gemäß der ermittelten Sicherheitskonfiguration eingestellt werden (Schritt 204).

Anschließend wird das Verfahren beendet (Schritt 205).

Der in dem Ablaufdiagramm 200 dargestellte Programmablauf kann einmal oder auch wiederholt von dem PDA 100 durchgeführt werden.

Vorzugsweise wird das dargestellte Verfahren bei einer Änderung der aktuellen Einsatzumgebung durchgeführt.

Fig.3 zeigt eine Kommunikationseinrichtung 300 gemäß einem zweiten Ausführungsbeispiel der Erfindung.

Dargestellt ist eine auf einem Bildschirm 301 dargestellte graphische Bildschirmoberfläche, mittels der eine Mehrzahl von unterschiedlichen Einsatzumgebung zur manuellen Auswahl durch den Benutzer des Kommunikationsgerät 300 dargestellt werden, gemäß diesem Ausführungsbeispiel die oben beschriebenen Einsatzumgebungen, nämlich eine erste Einsatzumgebung 302 [Firma-Wireless], eine zweite Einsatzumgebung 303 [Firma-DirektPC], eine dritte Einsatzumgebung 304 [Heim] sowie eine vierte Einsatzumgebung 305 [Rest].

Ferner sind auf dem berührungssensitiven Bildschirm (Touchscreen) 301 in einem anderen Fenster 306 Steuerknöpfe 307, 308, 309, 310 zur Auswahl durch den Benutzer dargestellt.

Durch Auswahl der gewünschten Einsatzumgebung 302, 303, 304, 305 und durch Aktivierung der ersten Schaltfläche 307 "Aktiviere" kann ein Benutzer der Kommunikationseinrichtung 300 die der ausgewählten Einsatzumgebung 302, 303, 304, 305 zugeordnete Sicherheitskonfiguration aktivieren. In diesem Fall besteht eine 1:1-Zuordnung zwischen der jeweiligen Einsatzumgebung und der diesen Einsatzumgebung zugeordneten Sicherheitskonfiguration. Diese 1:1-Zuordnung ist in einer Zuordnungstabelle 103 gespeichert.

Ferner sind auf der Bildschirmoberfläche noch eine zweite Schaltfläche 308 ("Neu") zum Anlegen beziehungsweise zum Definieren einer neuen Einsatzumgebung, eine dritte Schaltflä-

che 309 ("Ändere") zum Ändern einer der vorgegebenen Einsatzumgebungen beziehungsweise derer Eigenschaften sowie eine vierte Schaltfläche 310 ("Lösche") zum Löschen einer der gespeicherten und dem Benutzer dargestellten Einsatzumgebungen.

Die Sicherheitskonfigurationen gemäß diesem Ausführungsbeispiel entsprechen den Sicherheitskonfigurationen gemäß dem oben beschriebenen Ausführungsbeispiel und werden aus diesem Grund hier nicht weiter erläutert.

Es ist in diesem Zusammenhang anzumerken, dass grundsätzlich eine beliebige Sicherheitskonfiguration definiert und vorgesehen sein kann, wobei die Sicherheitskonfigurationen unter Verwendung der üblichen und an sich bekannten Konfigurationen einer "Personal Firewall" erfolgen kann. Beispielsweise können erfindungsgemäß unter dem Betriebssystem Linux und anderen gängigen Unix-Systemen an sich bekannte host-basierte Paketfilter erfindungsgemäß eingesetzt werden.

In diesem Dokument sind folgende Veröffentlichungen zitiert:

[1] US 6321334 B1;

[2] US 6308273 B1;

[3] WO 01/82562 A2;

[4] EP 1 139 681 A1;

[5] M.S. Gast, 802.11 Wireless Networks: The Definite Guide, Creating and administrating Wireless Networks, ISBN 0-596-00183-5, 1. Auflage, Seiten 214 bis 235, April 2002.

Patentansprüche

1. Kommunikationseinrichtung,
- mit einer Einsatzumgebungs-Ermittlungseinrichtung, die eingerichtet ist zum Ermitteln einer Einsatzumgebung, in der die Kommunikationseinrichtung eingesetzt wird,
- mit einer Kommunikationsschnittstelle, eingerichtet zur Kommunikation der Kommunikationseinrichtung mit einer anderen Kommunikationseinrichtung,
- mit einem Sicherheitskonfigurations-Speicher, in dem eine Mehrzahl unterschiedlicher Sicherheitskonfigurationen hinsichtlich des Betriebs der Kommunikationseinrichtung gespeichert sind,
- mit einer Sicherheitskonfigurations-Ermittlungseinrichtung, welche derart eingerichtet ist, dass unter Verwendung der ermittelten Einsatzumgebung eine zugehörige Sicherheitskonfiguration aus der Mehrzahl von Sicherheitskonfigurationen ermittelt wird,
- mit einer Sicherheitskonfigurations-Einstelleinrichtung, welche eingerichtet ist zum Einstellen der Sicherheitskonfiguration der Kommunikationseinrichtung gemäß der von der Sicherheitskonfigurations-Ermittlungseinrichtung ermittelten Sicherheitskonfiguration.

2. Kommunikationseinrichtung gemäß Anspruch 1, eingerichtet als mobile Kommunikationseinrichtung.

3. Kommunikationseinrichtung gemäß Anspruch 2, eingerichtet als zumindest eine der folgenden Kommunikationseinrichtungen:
- ein Mobilfunktelefon;
- ein Schnurlostelefon;
- ein persönlicher Digitaler Assistent;
- ein Pager; und/oder
- ein tragbarer Computer.

4. Kommunikationseinrichtung gemäß einem der Ansprüche 1 bis 3,
bei der die Kommunikationsschnittstelle eingerichtet ist
- als eine Kommunikationsschnittstelle zur Kommunikation mit einem Personal Computer;
- als eine Modem-Kommunikationsschnittstelle;
- als eine ISDN-Adapter-Kommunikationsschnittstelle; und/oder
- als eine LAN-Adapter-Kommunikationsschnittstelle.

5. Kommunikationseinrichtung gemäß einem der Ansprüche 1 bis 3,
bei der die Kommunikationsschnittstelle eingerichtet ist als Funk-Kommunikationsschnittstelle.

6. Kommunikationseinrichtung gemäß Anspruch 5,
bei der die Kommunikationsschnittstelle eingerichtet ist
- als eine Wireless-LAN-Kommunikationsschnittstelle;
- als eine Schnurlos-Kommunikationsschnittstelle; und/oder
- als eine Mobilfunk-Kommunikationsschnittstelle.

7. Kommunikationseinrichtung gemäß einem der Ansprüche 1 bis 6,
mit einem Zuordnungstabellen-Speicher, in dem eine Zuordnungstabelle gespeichert ist, wobei in der Zuordnungstabelle zu einer Einsatzumgebung jeweils mindestens eine Sicherheitskonfiguration zugeordnet ist.

8. Kommunikationseinrichtung gemäß einem der Ansprüche 1 bis 7,
bei der die Einsatzumgebungs-Ermittlungseinrichtung eine Einsatzumgebungs-Erfassungseinrichtung aufweist, die eingerichtet ist zum automatischen Erfassen und Bestimmen der Einsatzumgebung der Kommunikationseinrichtung.

9. Kommunikationseinrichtung gemäß Anspruch 8,

bei der die Einsatzumgebungs-Erfassungseinrichtung eingerichtet ist zum Erfassen eines oder mehrerer von der Kommunikationseinrichtung verwendeter Kommunikationsverfahren und/oder zum Erfassen eines oder mehrerer von der Kommunikationseinrichtung im Rahmen einer Kommunikation verwendeter Sicherheitsmechanismen.

10. Kommunikationseinrichtung gemäß Anspruch 9,
bei der die Einsatzumgebungs-Erfassungseinrichtung eingerichtet ist zum Erfassen eines oder mehrerer von der Kommunikationseinrichtung im Rahmen einer Kommunikation verwendeter Sicherheitsmechanismen, wobei zumindest einer der folgenden Sicherheitsmechanismen berücksichtigt wird:
- ein Authentisierungsverfahren;
- eine Identifizierungsinformation zur Identifikation einer Kommunikationseinrichtung oder eines Teilnehmers;
- ein Schlüsselaustauschverfahren zum Austauschen kryptographischer Schlüssel;
- ein im Rahmen der Kommunikation verwendeter kryptographischer Schlüssel; und/oder
- im Rahmen der Kommunikation verwendete Informationselemente.

11. Kommunikationseinrichtung gemäß einem der Ansprüche 1 bis 10,
bei der die Einsatzumgebungs-Erfassungseinrichtung derart eingerichtet ist, dass zumindest eine der folgenden Einsatzumgebungen berücksichtigt werden kann:
- ein eigenes Firmen-Kommunikationsnetz;
- ein fremdes Kommunikationsnetz;
- das Heimat-Kommunikationsnetz eines Benutzers;
- das Heimat-Kommunikationsnetz eines Dritten;
- das Öffentliche Kommunikationsnetz; und/oder
- ein Ad-Hoc-Kommunikationsnetz.

12. Kommunikationseinrichtung gemäß einem der Ansprüche 1 bis 11,

bei der in einer Sicherheitskonfiguration Informationen über zumindest einen Teil der folgenden Aspekte enthalten ist:

- Information über ein oder mehrere von der Kommunikationseinrichtung nutzbare Kommunikationsprotokolle;
- Information über einen oder mehrere von der Kommunikationseinrichtung erreichbare Ziel-Kommunikationseinrichtungen;
- Information über von der Kommunikationseinrichtung ausführbare oder aufrufbare Computerprogramme oder Computerprogramm-Funktionen;
- Information über im Rahmen der Kommunikation von der Kommunikationseinrichtung zu verwendende Sicherheitsverfahren;
- Information über von der Kommunikationseinrichtung zugreifbare Daten;
- Information über von der Kommunikationseinrichtung gleichzeitig nutzbare Kommunikationsverfahren;
- Information über für die Kommunikationseinrichtung zugelassene Sicherheitsverfahren, verbotene Sicherheitsverfahren und/oder erforderliche Sicherheitsverfahren.

13. Verfahren zum Einstellen einer Sicherheitskonfiguration einer Kommunikationseinrichtung,

- bei dem eine Einsatzumgebung ermittelt wird, in der die Kommunikationseinrichtung eingesetzt wird,
- bei dem aus einer Mehrzahl in einem Sicherheitskonfigurations-Speicher gespeicherter unterschiedlicher Sicherheitskonfigurationen hinsichtlich des Betriebs der Kommunikationseinrichtung unter Verwendung der ermittelten Einsatzumgebung eine zugehörige Sicherheitskonfiguration ermittelt wird,
- bei dem die Kommunikationseinrichtung gemäß der ermittelten Sicherheitskonfiguration eingestellt wird.

Zusammenfassung

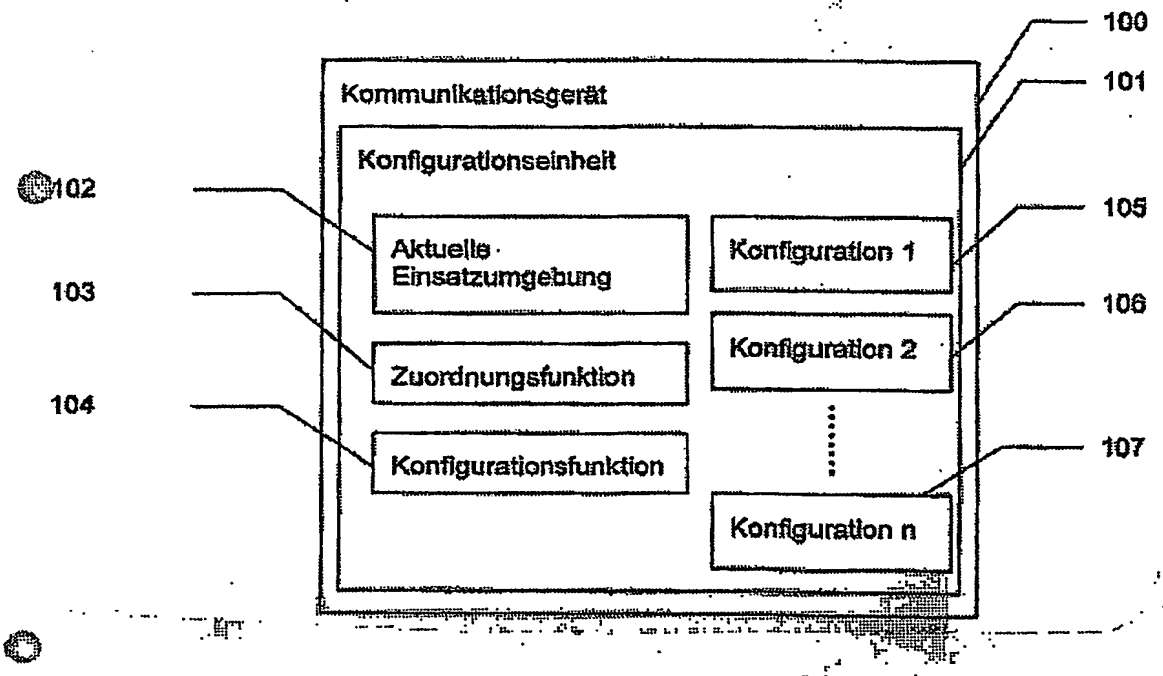
Kommunikationseinrichtung und Verfahren zum Einstellen einer Sicherheitskonfiguration einer Kommunikationseinrichtung

Nach erfolgter Ermittlung einer Einsatzumgebung der Kommunikationseinrichtung wird aus einer Mehrzahl gespeicherter Sicherheitskonfigurationen eine Sicherheitskonfiguration ausgewählt und die Kommunikationseinrichtung wird gemäß der ausgewählten Sicherheitskonfiguration konfiguriert.

Signifikante Figur 1

2003 P 03868

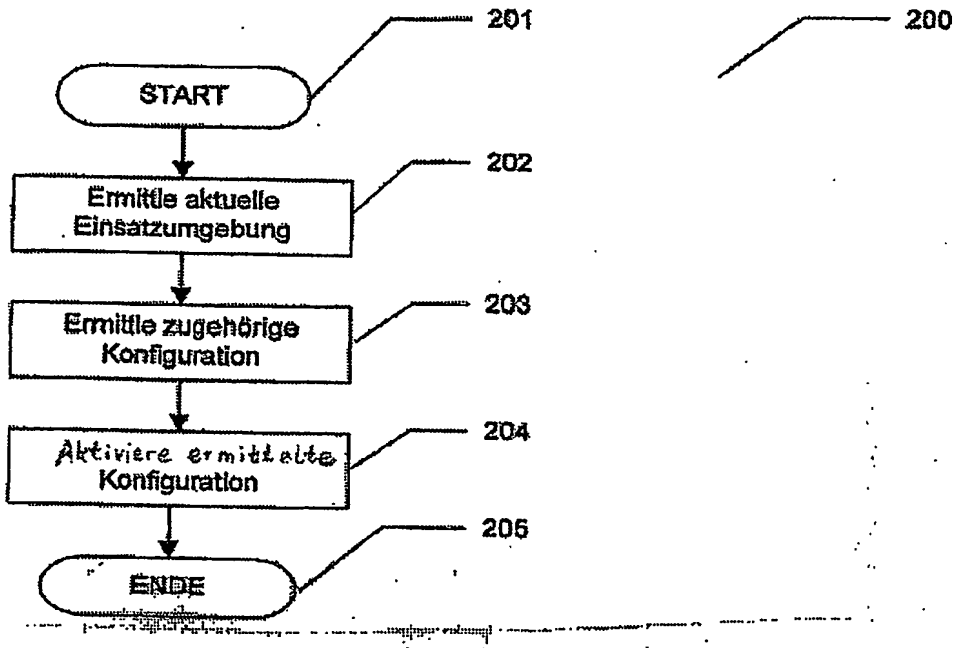
FIG 1



2003 P 03868

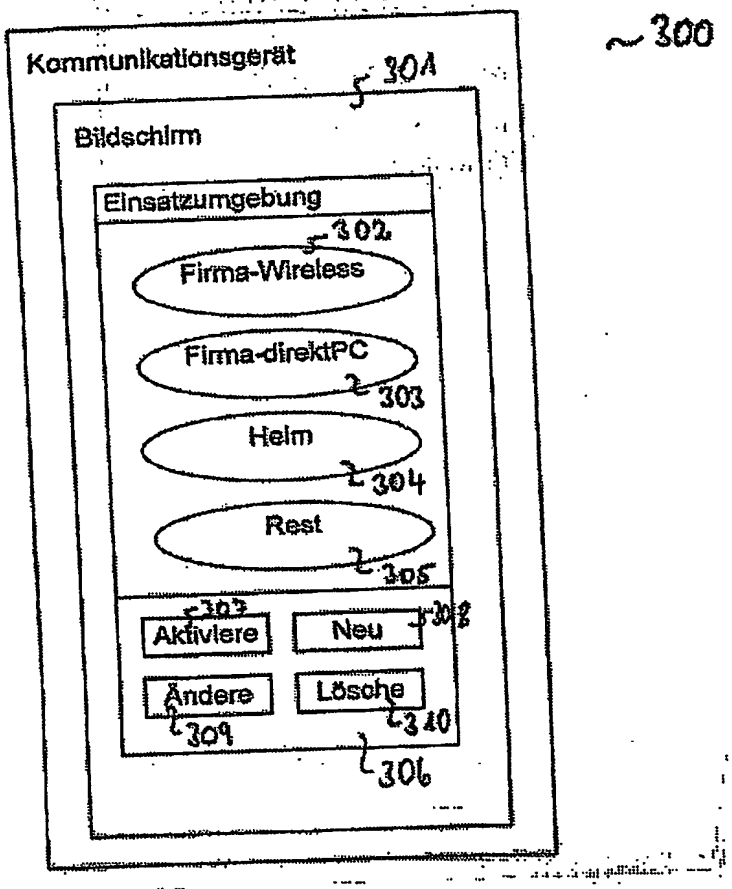
2/3

FIG 2



2003P03868

FIG 3



This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☑ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.